Posudek vedoucího diplomové práce

Název: Kryptosystémy založené na teorii kódů
Autor: Zuzana Parýzková

Tématem předložené práce je důkladný matematický popis nejvýznamnějších kryptografických protokolů založených na teorii lineárních blokových kódů spolu s vysvětlením možných útoků na tyto protokoly a obrany proti nim. Vedle standardního McElieceova a Niederreiterova schématu se jedná především o jejich Gabidulinovu variantu využívající hodnostní metriky.

Práce sestává z úvodu, pěti kapitol, závěru a přílohy obsahující výpočet příkladu Sidelnikovova-Shestakovova útoku. Zatímco stručná první kapitola práce shrnuje potřebnou terminologii a její základní vlastnosti, detailnímu vysvětlení klasického McElieceova a Niederreiterova schématu se věnuje kapitola bezprostředně následující. Pravděpodobnostní Sternův útok na obě schémata je obsahem třetí kapitoly, její jádro tvoří důkaz korektnosti algoritmu, který hledá kódové slovo zadané váhy. Nejrozsáhlejší část práce představuje čtvrtá kapitola prezentující Sidelnikovovův-Shestakovův útok. Hlavním výsledkem je zde detailní důkaz klasického Sidelnikovova-Shestakovova útoku na Niederreiterovo schéma založené na zobecněných Reedových-Solomonových kódech, včetně konstrukce ilustračního hračkového příkladu. Pátá sekce práce je věnována variantám obou popisovaných kryptosystémů nad Gabidulinovými kódy. Kromě matematického oprávnění obou variant kapitola nastiňuje fungování Overbeckova útoku na Gabidulinovu variantu McElieceova schématu a v návaznosti na ní popisuje nový útok na variantu tohoto schématu bez maskovací matice.

Byť základ práce tvoří kompilace známých výsledků o klasických kryptosystémech a útocích na ně, je podstatná část matematického odůvodnění výsledkem samostatné práce motivované přílišným nadhledem dostupných textů k tomuto tématu. Vlastním autorčiným výsledkem je vedle konstrukce několika příkladů především útok Gabidulinovu variantu McElieceova schématu bez maskovací matice, který dokládá bezpečnostní nezbytnost využití této matice. Prezentovaný útok využívá některé nápady pocházející z Overbeckova útoku nikoli ovšem (pravděpodobně nesprávnou) Overbeckovu domněnku, že by podobný útok měl být realizovatelný adaptováním myšlenek Sidelnikovova-Shestakovova útoku.

Text je napsán velmi přehledně a pečlivě. Velmi dobře se čte a po matematické ani jazykové stránce se mu podle mého mínění nedá nic podstatného vytknout. Všechny nedostatky či nepřesnosti, kterých jsem si povšiml v pracovních verzích práce, autorka k mé spokojenosti opravila, proto k finální podobě textu již žádné připomínky nemám. Práce bez nejmenší pochyby svědčí o autorčině vhledu do zkoumané problematiky i o její schopnosti samostatné odborné práce.

Z uvedených důvodů se domnívám, že práce Zuzany Parýzkové *Kryptosystémy založené na teorii kódů* úspěšně naplnila zadání, a bez výhrad ji doporučuji uznat jako diplomovou.

Jan Žemlička
Katedra algebry
26.1.2023